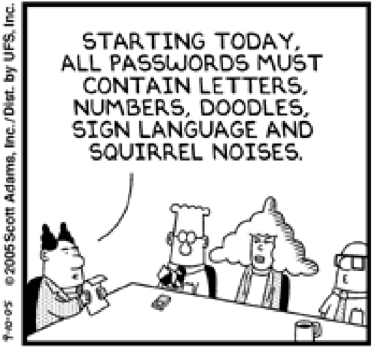
Cryptography: Key Issues in Security

L. Babinkostova J. Keller B. Schreiner
J. Schreiner-McGraw K. Stubbs

August 1, 2014

Motivation


STARTING TODAY, ALL PASSWORDS MUST CONTAIN LETTERS, NUMBERS, DOODLES, SIGN LANGUAGE AND SQUIRREL NOISES.
© 2005 Scott Adams, Inc./Dist. by UFS, Inc.

General Cryptosystems

Definition

A *cryptosystem* is an ordered 4-tuple $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{T})$ where $\mathcal{M}$, $\mathcal{C}$, and $\mathcal{K}$ are called the *message space*, the *ciphertext space*, and the *key space* respectively, and where $\mathcal{T} : \mathcal{M} \times \mathcal{K} \to \mathcal{C}$ is a transformation such that for each $k \in \mathcal{K}$, the mapping $\mathcal{T}[k] : \mathcal{M} \to \mathcal{C}$, called an encryption transformation, is invertible.

General Cryptosystems

Definition

A *cryptosystem* is an ordered 4-tuple $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{T})$ where $\mathcal{M}$, $\mathcal{C}$, and $\mathcal{K}$ are called the *message space*, the *ciphertext space*, and the *key space* respectively, and where $\mathcal{T} : \mathcal{M} \times \mathcal{K} \to \mathcal{C}$ is a transformation such that for each $k \in \mathcal{K}$, the mapping $\mathcal{T}[k] : \mathcal{M} \to \mathcal{C}$, called an encryption transformation, is invertible.

For any cryptosystem $\Pi = (\mathcal{M}, \mathcal{C}, \mathcal{K}, T)$, let $\mathcal{T}_\Pi = \{\mathcal{T}[k] : k \in \mathcal{K}\}$ be the set of all encryption transformations.

General Cryptosystems

Definition

A *cryptosystem* is an ordered 4-tuple $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{T})$ where $\mathcal{M}$, $\mathcal{C}$, and $\mathcal{K}$ are called the *message space*, the *ciphertext space*, and the *key space* respectively, and where $\mathcal{T} : \mathcal{M} \times \mathcal{K} \to \mathcal{C}$ is a transformation such that for each $k \in \mathcal{K}$, the mapping $\mathcal{T}[k] : \mathcal{M} \to \mathcal{C}$, called an encryption transformation, is invertible.

For any cryptosystem $\Pi = (\mathcal{M}, \mathcal{C}, \mathcal{K}, T)$, let $\mathcal{T}_\Pi = \{\mathcal{T}[k] : k \in \mathcal{K}\}$ be the set of all encryption transformations.

Definition

The symbol $\mathcal{G} = \langle \mathcal{T}_\Pi \rangle$ denotes group that is generated by the set $\mathcal{T}_\Pi$.

Group Generated by One Round Function

Definition

Let $T[k]$ denote the round function of the cipher under the key $k \in \mathcal{K}$, where $\mathcal{K}$ denotes the set of all round keys.

Group Generated by One Round Function

Definition

Let $T[k]$ denote the round function of the cipher under the key $k \in \mathcal{K}$, where $\mathcal{K}$ denotes the set of all round keys.

Definition

Let $L = \{T[k] | k \in \mathcal{K}\}$ be the set of all round functions.

Group Generated by One Round Function

Definition

Let $T[k]$ denote the round function of the cipher under the key $k \in \mathcal{K}$, where $\mathcal{K}$ denotes the set of all round keys.

Definition

Let $L = \{T[k] | k \in \mathcal{K}\}$ be the set of all round functions.

Definition

We denote $\mathcal{G}_T = \langle \{T[k] | k \in \mathcal{K}\} \rangle$ generated by these permutations.

Key Schedule

Definition

An s-round cipher has key schedule $KS : \mathcal{K} \to \mathcal{K}^s$ so that any key $k \in \mathcal{K}$ produces a set of subkeys $k_i \in \mathcal{K}$, $1 \leq i \leq s$.

Key Schedule

Definition

An s-round cipher has key schedule $KS : \mathcal{K} \to \mathcal{K}^s$ so that any key $k \in \mathcal{K}$ produces a set of subkeys $k_i \in \mathcal{K}$, $1 \leq i \leq s$.

Definition

The group $\mathcal{G}_T^s = \langle T[k_s]T[k_{s-1}] \cdots T[k_1] | k_i \in \mathcal{K} \rangle$ is the group generated by s round functions (independently chosen).

Relation between these groups

$$\mathcal{G}_T = \langle T[k] | k \in \mathcal{K} \rangle$$

$$\mathcal{G}_T^s = \langle T[k_s]T[k_{s-1}] \cdots T[k_1] | k_i \in \mathcal{K} \rangle$$

$$\mathcal{G} = \langle T[k_s]T[k_{s-1}] \cdots T[k_1] | KS(k) = (k_1, k_2, \cdots, k_s) \rangle$$

Relation between these groups

$$\mathcal{G}_T = \langle T[k] | k \in \mathcal{K} \rangle$$

$$\mathcal{G}_T^s = \langle T[k_s]T[k_{s-1}] \cdots T[k_1] | k_i \in \mathcal{K} \rangle$$

$$\mathcal{G} = \langle T[k_s]T[k_{s-1}] \cdots T[k_1] | KS(k) = (k_1, k_2, \cdots, k_s) \rangle$$

$$\mathcal{G} = \langle \mathcal{T}_\Pi \rangle$$

Relation between these groups

$$\mathcal{G}_T = \langle T[k] | k \in \mathcal{K} \rangle$$

$$\mathcal{G}_T^s = \langle T[k_s]T[k_{s-1}] \cdots T[k_1] | k_i \in \mathcal{K} \rangle$$

$$\mathcal{G} = \langle T[k_s]T[k_{s-1}] \cdots T[k_1] | KS(k) = (k_1, k_2, \cdots, k_s) \rangle$$

$$\mathcal{G} = \langle \mathcal{T}_\Pi \rangle$$

$$\mathcal{G} \subset \mathcal{G}_T^s \trianglelefteq \mathcal{G}_T$$

Primitivity

Definition

Recall that a group action on a set V is transitive if

$$\forall x, y \in V,\ \exists g \in G \text{ s.t. } xg = y.$$

Primitivity

Definition

Recall that a group action on a set V is transitive if

$$\forall x, y \in V, \ \exists g \in G \text{ s.t. } xg = y.$$

Definition

A transitive group G is imprimitive in its action on V if there exists a non-trivial partition $\mathcal{B}$ of V (i.e. $\mathcal{B} \neq \{V\}$, $\mathcal{B} \neq \{\{v\} \mid v \in V\}$) such that $Bg \in \mathcal{B}$, $\forall B \in \mathcal{B}$ and $\forall g \in G$. We call such a $\mathcal{B}$ a block system for G. A group action is primitive if it is not imprimitive.

Examples of Block Systems

Example

$T(\mathbb{Z}_n)$, the group of translations on $\mathbb{Z}_n$, where $x \mapsto a + x \pmod{n}$ has as many block systems as there are factorizations of n into two integers a and b, both greater than 1.

Examples of Block Systems

Example

$T(\mathbb{Z}_n)$, the group of translations on $\mathbb{Z}_n$, where $x \mapsto a + x \pmod{n}$ has as many block systems as there are factorizations of n into two integers a and b, both greater than 1.

Example

The subgroup of the symmetric group on $S = \{1, 2, 3, 4\}$, $\langle\sigma\rangle$, where $\sigma = (1234)$, is imprimitive. A block system $\mathcal{B}$ is $\{\{1, 3\}, \{2, 4\}\}$.

Our Questions

- Is the set of encryption functions a group?

Our Questions

- Is the set of encryption functions a group?
- When is the group generated transitive?

Our Questions

- Is the set of encryption functions a group?
- When is the group generated transitive?
- When is the group generated primitive?

Our Questions

- Is the set of encryption functions a group?
- When is the group generated transitive?
- When is the group generated primitive?
- When is the group generated by the encryption functions the symmetric or alternating group?

Notation

- Message Space: $r, m, n \in \mathbb{Z}^+$, $\mathcal{M} = \mathrm{GF}(p^{rmn}) \cong (\mathrm{GF}(p^r))^{mn}$

Notation

- Message Space: $r, m, n \in \mathbb{Z}^+$, $\mathcal{M} = \mathrm{GF}(p^{rmn}) \cong (\mathrm{GF}(p^r))^{mn}$
- Internal Representation: $t : (\mathrm{GF}(p^r))^{mn} \to M_{m,n}(\mathrm{GF}(p^r))$

$$t : [a_1, \ \dots \ , \ a_{mn}] \mapsto \begin{bmatrix} a_1 & a_2 & \dots & a_n \\ a_{n+1} & a_{n+2} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{(m-1)n} & a_{(m-1)n+1} & \dots & a_{mn} \end{bmatrix}.$$

Theorem

Let $\mathcal{C}$ be a translation-based cipher over $\mathbb{F}_q$, and suppose that the h-th round is proper. If each brick of γ_h is

1. *weakly p^r-uniform, and*
2. *strongly r-anti-invariant*

then the group generated by $\mathcal{C}$ is primitive.

Theorem

Let $\mathcal{C}$ be a translation-based cipher such that

1. *$\mathcal{C}$ satisfies the hypotheses of the above theorem, and*
2. *for all $0 \neq a \in V_i$, $\{(x+a)\gamma_i - x\gamma_i | x \in V_i\}$ is not a coset of a subgroup of V_i*

then the group generated by $\mathcal{C}$ is either Alt(V) or Sym(V).

R. Aragona, A. Caranti, F. Dalla Volta, and M. Sala, *On the group generated by round functions of translation based ciphers over arbitrary finite fields*, **Elsevier**, (2013).

Definition

An element $\gamma \in \mathrm{Sym}(V)$ is called a bricklayer transformation with respect to $V = V_1 \oplus \cdots \oplus V_n$ if γ acts on an element $v = v_1 + \cdots + v_n$ with $v_i \in V_i$ as $v\gamma = v_1\gamma_1 + \cdots + v_n\gamma_n$ for some $\gamma_i \in \mathrm{Sym}(V)$.

Definition

Let $\psi \in \mathrm{GL}(V)$ be a linear map. Then ψ is called a mixing layer. If ψ leaves no sum $\oplus V_i$ invariant, then ψ is called a proper mixing layer.

- Key Schedule: $KS : \mathcal{K} \to \mathcal{K}^s$.
- Key Mapping: $\phi(k, h) : \mathcal{K} \times \{1, \ldots, s\} \to \mathcal{M}$.

- Key Schedule: $KS : \mathcal{K} \to \mathcal{K}^s$.
- Key Mapping: $\phi(k,h) : \mathcal{K} \times \{1,\ldots,s\} \to \mathcal{M}$.
- In both cases the key k is called the **master key**.

A block cipher $\mathcal{C} = \{\tau_k : k \in \mathcal{K}\}$ over $\mathbb{F}_q$ is **translation based (tb)** if

1. each τ_k is the composition of h round functions $\tau_{k,h}$, and $h = 1, \dots, s$ where in turn each round function can be written as a composition $\sigma_{\phi(k,h)} \circ \psi_h \circ \gamma_h$ of three permutations of V, where
   - γ_h is a bricklayer transformation not depending on k and with $0\gamma_h = 0$,
   - ψ_h is a linear transformation not depending on k,
   - $\phi : \mathcal{K} \times \{1, \dots, s\} \to V$ is the key schedule
2. for one round h_0
   - ψ_{h_0} is a proper mixing layer, and
   - the map $\mathcal{K} \to V$ by $k \mapsto \phi(k, h_0)$ is surjective on V.

AES as a tb cipher

For reference a single round of AES is the following composition of functions:

$$\sigma_k \circ \rho \circ \pi \circ \lambda$$

Recall, our definition of tb cipher had three components:

AES as a tb cipher

For reference a single round of AES is the following composition of functions:

$$\sigma_k \circ \rho \circ \pi \circ \lambda$$

Recall, our definition of tb cipher had three components:

- A bricklayer transformation.

AES as a tb cipher

For reference a single round of AES is the following composition of functions:

$$\sigma_k \circ \rho \circ \pi \circ \lambda$$

Recall, our definition of tb cipher had three components:

- A bricklayer transformation.
- A mixing layer.

AES as a tb cipher

For reference a single round of AES is the following composition of functions:

$$\sigma_k \circ \rho \circ \pi \circ \lambda$$

Recall, our definition of tb cipher had three components:

- A bricklayer transformation.
- A mixing layer.
- A surjective key schedule.

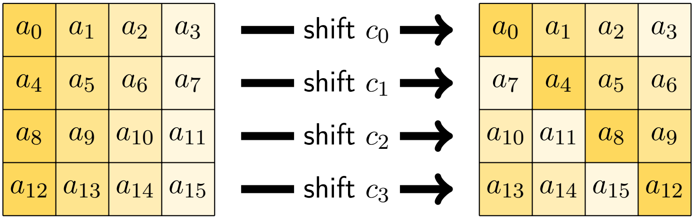
SubBytes, λ

a_0	a_1	a_2	a_3
a_4	a_5	a_6	a_7
a_8	a_9	a_{10}	a_{11}
a_{12}	a_{13}	a_{14}	a_{15}

a'_0	a'_1	a'_2	a'_3
a'_4	a'_5	a'_6	a'_7
a'_8	a'_9	a'_{10}	a'_{11}
a'_{12}	a'_{13}	a'_{14}	a'_{15}

$$a_i \mapsto A a_i^{-1} + B$$

ShiftRows, π



MixColumns, ρ

$$\begin{bmatrix} c_0 & c_1 & c_2 & c_3 \\ c_1 & c_2 & c_3 & c_0 \\ c_2 & c_3 & c_0 & c_1 \\ c_3 & c_0 & c_1 & c_2 \end{bmatrix} \otimes \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 & a_7 \\ a_8 & a_9 & a_{10} & a_{11} \\ a_{12} & a_{13} & a_{14} & a_{15} \end{bmatrix} = \begin{bmatrix} a'_0 & a'_1 & a'_2 & a'_3 \\ a'_4 & a'_5 & a'_6 & a'_7 \\ a'_8 & a'_9 & a'_{10} & a'_{11} \\ a'_{12} & a'_{13} & a'_{14} & a'_{15} \end{bmatrix}$$

AddRoundKey, σ_k

$$\begin{array}{|c|c|c|c|}\hline a_{15} & a_{11} & a_7 & a_3 \\ \hline a_{14} & a_{10} & a_6 & a_2 \\ \hline a_{13} & a_9 & a_5 & a_1 \\ \hline a_{12} & a_8 & a_4 & a_0 \\ \hline \end{array} \bigoplus \begin{array}{|c|c|c|c|}\hline k_0 & k_1 & k_2 & k_3 \\ \hline k_4 & k_5 & k_6 & k_7 \\ \hline k_8 & k_9 & k_{10} & k_{11} \\ \hline k_{12} & k_{13} & k_{14} & k_{15} \\ \hline \end{array} = \begin{array}{|c|c|c|c|}\hline a'_0 & a'_1 & a'_2 & a'_3 \\ \hline a'_4 & a'_5 & a'_6 & a'_7 \\ \hline a'_8 & a'_9 & a'_{10} & a'_{11} \\ \hline a'_{12} & a'_{13} & a'_{14} & a'_{15} \\ \hline \end{array}$$

Proper Mixing Layer

Definition

A linear map ψ is a proper mixing layer if it leaves no nontrivial, nonzero subspace W of V invariant, where $W = \bigoplus_{i \in I} V_i$,
$V = \mathcal{M}_{m,n}(\mathrm{GF}(p^r)) = V_1 \oplus \cdots \oplus V_{mn}$, and $I \subsetneq \{1, \ldots, mn\}$.

ShiftRows Conditions

Theorem

The composition $\rho \circ \pi$ is a proper mixing layer if and only if ρ properly mixes columns and for all $k \in (1, \ldots, n-1)$, there exists some c_i such that $j_a \cdot c_a + \cdots + j_b \cdot c_b \equiv_n k$ for $j_i \in \mathbb{N}$.

MixColumns Conditions

Theorem

Let $C \in M_{m,m}GF(p^r)$ *be a circulant matrix with first row* $[c_1, c_2, \ldots, c_m]$ *such that the only nonzero terms are indexed* c_{i+1} *for* $i \in I = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$*. Then* C *is a proper mixing matrix if and only if* $< I >= \mathbb{Z}_m$*.*

MixColumns Conditions

Theorem

Let $C \in M_{m,m}GF(p^r)$ *be a circulant matrix with first row* $[c_1, c_2, \ldots, c_m]$ *such that the only nonzero terms are indexed* c_{i+1} *for* $i \in I = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$. *Then* C *is a proper mixing matrix if and only if* $< I >= \mathbb{Z}_m$.

Example

Example on Board

Non-Surjective Key Schedules

- Instead of surjectivity, we actually need $T(V) \subset \langle T_s[k] : k \in \mathcal{K} \rangle$.

Theorem

If the key mapping function is onto a set of generators and the zero key, then $T(V) \subset \langle T_s[k] : k \in \mathcal{K} \rangle$.

Conjecture

If $T_s[k]$ *is a generlized AES cipher with a proper mixing layer than the converse holds.*

Implications and future work

- Analyze existing hash functions based on AES.

Implications and future work

- Analyze existing hash functions based on AES.
- Construct future ciphers over more complicated fields.

Implications and future work

- Analyze existing hash functions based on AES.
- Construct future ciphers over more complicated fields.
- Prove the Non-surjectivity conjecture.

Implications and future work

- Analyze existing hash functions based on AES.
- Construct future ciphers over more complicated fields.
- Prove the Non-surjectivity conjecture.
- Analyze the effects of using a Mixing Matrix with zero entries.

Implications and future work

- Analyze existing hash functions based on AES.
- Construct future ciphers over more complicated fields.
- Prove the Non-surjectivity conjecture.
- Analyze the effects of using a Mixing Matrix with zero entries.
- Analyze the effects of using a key schedule surjective onto generators.

Acknowledgements

Boise State University and NSF DMS 1359425

References

R. Aragona, A. Caranti, F. Dalla Volta, and M. Sala, *On the group generated by the round functions of translation based ciphers over arbitrary finite fields*, **Finite Fields and Their Applications**, Vol. 25 293-305, (2014).

L. Babinkostova, K. Bombardier, M. Cole, T. Morrell, and C. Scott, *Algebraic Structure of generalized Rijndael-like SP networks*, **Groups Complexity Cryptology**, Vol. 6 Issue 1 37-54, (2014)

R. Sparr, R. Wernsdorf, *Group Theoretic Properties of Rijndael-like Ciphers*, **Discrete Applied Mathematics**, 156(16): 3139-3149 (2008)